BEAVERTON POLICE DEPARTMENT

GENERAL ORDER

NUMBER: 15.03.00
SUBJECT: ELECTRONIC MESSAGING
EFFECTIVE: AUGUST 1, 1999
REVIEW: AUGUST 2001, 2003, 2005, 2007

1. PURPOSE. It is the purpose of this policy to provide officers with guidance on the proper use of personal computers and related electronic messaging systems utilized in this department for purposes of disseminating electronic mail, utilizing services of the Internet and related electronic message transmission, recording and storage devices.

2. POLICY**.** The availability and use of the personal computer within the work environment have provided many opportunities for enhancement of productivity and effectiveness. These technologies also entail the opportunity for rapid transfer and broad distribution of sensitive information that can also have damaging effects on this department, its members, and the public if not managed properly. Therefore, it is the policy of this department that all members abide by the guidelines set forth herein when using personal computers and the services of both internal and external databases and information exchange networks, and where applicable, voice mail, mobile digital terminals, and related electronic messaging devices.

3. DEFINITIONS**.** Electronic Messaging Device (EMD): For purposes of this order, electronic messaging devices include personal computers, electronic mail systems, voice mail systems, paging systems, electronic bulletin boards and Internet services, mobile digital terminals, and facsimile transmissions.

4. GENERAL**.**

A**.** Transmission of electronic messages and information on communications media provided for members of this department shall be treated with the same degree of propriety, professionalism, and confidentiality as official written correspondence or public records.

B**.** This department encourages authorized and trained personnel with access to EMDs to utilize these devices whenever necessary. However, use of any of

C. EMDs and their contents are the property of this department and intended for use in conducting official business with limited exceptions noted elsewhere in this order.

D. Members are advised that they do not maintain any right to privacy in EMD equipment or its contents, to include personally owned software.

1. The department reserves the right to access any information contained in EMDs and may require members to provide passwords to files that have been encrypted or password protected.

2. The department reserves the right to access, for quality control purposes and/or for violations of this policy, electronic and voice transmissions of members conducting business of this department.

E. Accessing or transmitting materials (other than that required for police business) that involves the use of obscene language, images, jokes, sexually explicit materials, or messages that disparage any person, group, or classification of individuals is prohibited whether or not a recipient has consented to or requested such material.

F. Confidential, proprietary, or sensitive information may be disseminated (or made available through shared directories or networked systems) only to individuals with a need and a right to know and when there is sufficient assurance that appropriate security of such information will be maintained. Such information includes but is not limited to the following:

1. Transmittal of personnel information, such as salary, performance reviews, complaints, grievances, misconduct, disciplinary information, medical records, or related employee information.

2. Criminal history information and confidential informant master files, identification files, or related information.

3. Intelligence files and information containing sensitive tactical and undercover information.

G. No member shall access or allow others to access any file or database unless that person has a need and a right to such information. Additionally, personal identification and access codes shall not be revealed to any unauthorized source.

H. An EMD is designed and intended to conduct business of this department and is restricted to that purpose. Installation of or access to software for purely entertainment purposes is prohibited. Exceptions to business use include the following:

1. Infrequent personal use of these devices may be permissible if limited in scope and frequency, if in conformance with other elements of this order, and if not connected with a profit-making business enterprise or the promotion of any product, service, or cause that has not received prior approval of this agency.

2. Personnel may make off-duty personal use of agency computers for professional and career development purposes when in keeping with other provisions of this policy and with prior knowledge of an appropriate supervisor.

5. IMPORTING/DOWNLOADING INFORMATION AND SOFTWARE.

A. Members shall not download or install on their personal computer or network terminal any file (including sound and video files and files attached to e-mail messages), software, or other materials from the Internet or other external sources without taking prescribed steps to preclude infection by computer viruses.

1. Material shall be downloaded to floppy drives and scanned for viruses prior to being entered into any personal or shared system.

2. In no case shall external materials or applications be downloaded directly to any shared (network) drive. When in doubt, members shall consult the system manager for guidance.

B. Members shall observe the copyright and licensing restrictions of all software applications and shall not copy software from internal or external sources unless legally authorized.

1. Any software for which proof of licensing (original disks, original manuals and/or license) cannot be provided is subject to removal by authorized agency personnel.

2. Privately owned software may not be loaded on agency computers.

C. Members shall observe copyright restrictions of any documents, images, or sounds sent through or stored on electronic mail.

D**.** Any hardware enhancements or additions to agency-owned equipment must be approved and authorized by the system administrator. The system administrator is responsible for determining proper installation procedures.

E**.** Members shall not permit unauthorized persons to use this agency's electronic mail system.

F. To avoid breaches of security, members shall log off any personal computer that has access to the agency's computer network, electronic mail system, the Internet, or sensitive information whenever they leave their work station.

_____ _____

Chief of Police Date